Learning with Errors, Circular Security & Fully Homomorphic Encryption

Daniele Micciancio (UCSD)
& Vinod Vaikuntanathan (MIT)

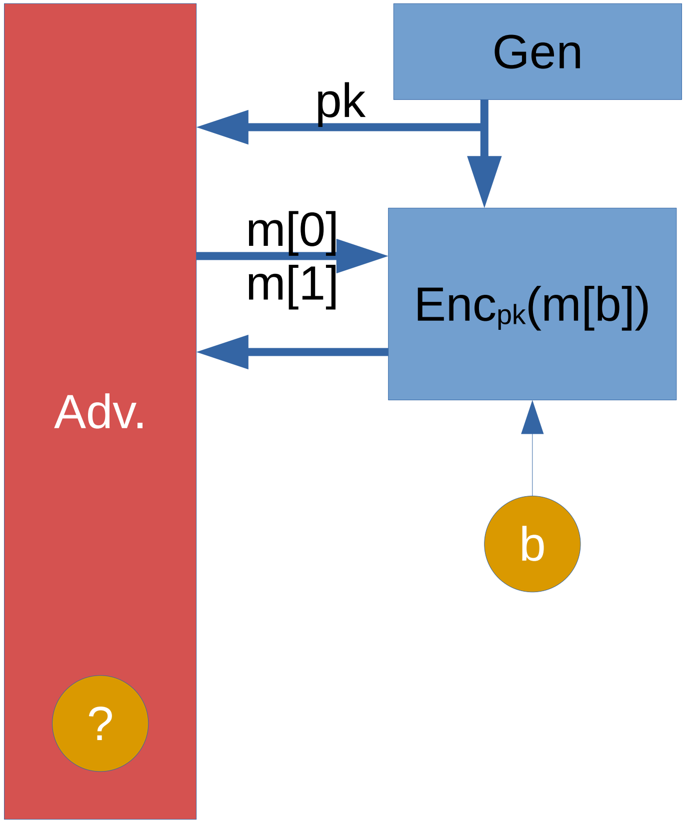
[PKC 2024]

Outline

- Introduction:
  - The problem: Encryption and circular security
  - Motivation: Fully Homomorphic Encryption (FHE)
- **Contributions:**
  - **Circular LWE assumption(s)**
  - **Example:** Search to decision reduction
- Conclusion and Open Problems

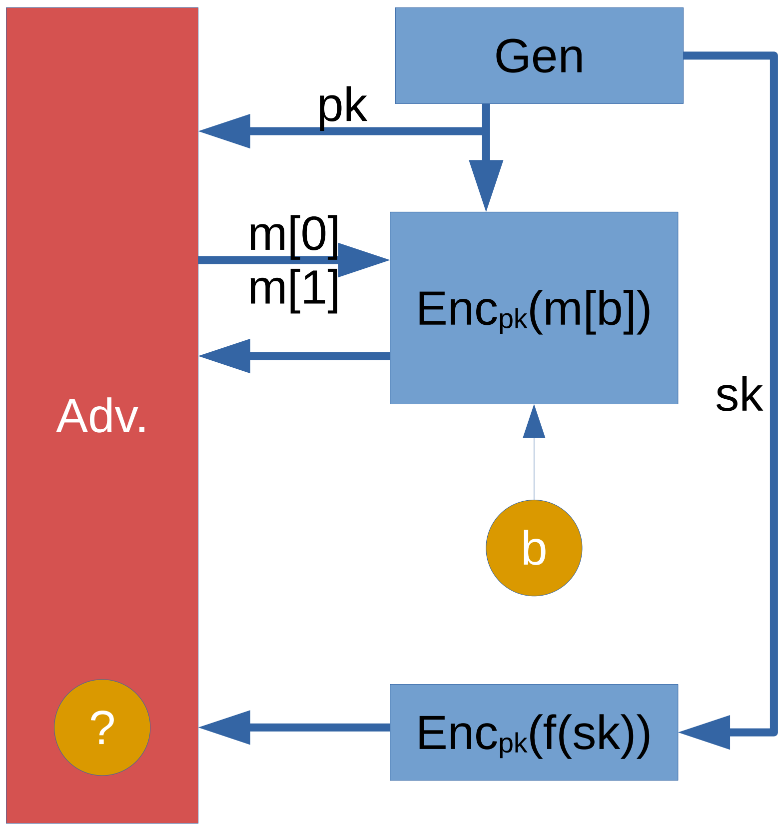
Security of Encryption

- Encryption scheme: (Gen,Enc,Dec)
- Semantic (IND-CPA) Security
  [Goldwasser,Micali'84]
  - $(pk,sk) \leftarrow Gen()$
  - $(pk,Enc_{pk}(m_0)) \approx (pk,Enc_{pk}(m_1))$
  - m_0,m_1 are adversarially chosen, but
  - cannot depend on the secret key sk
- Circular security: what if m=f(sk)?
  - [GM'84] already shows that some schemes may be broken



Security of Encryption

- Encryption scheme: (Gen,Enc,Dec)
- Semantic (IND-CPA) Security [Goldwasser,Micali'84]
  - $(pk,sk) \leftarrow Gen()$
  - $(pk,Enc_{pk}(m_0)) \approx (pk,Enc_{pk}(m_1))$
  - m_0,m_1 are adversarially chosen, but
  - cannot depend on the secret key sk
- Circular security: what if m=f(sk)?
  - [GM'84] already shows that some schemes may be broken



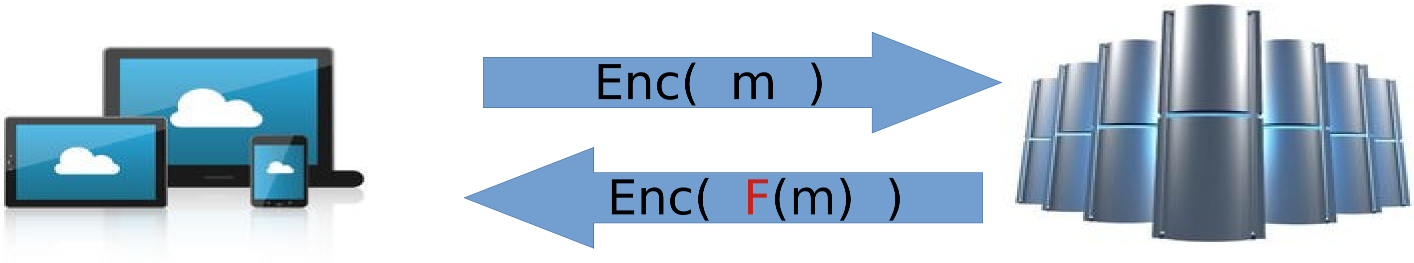
Circular Security: Motivation

- Full disk encryption
- Symbolic security analysis [Abadi,Rogaway'07,...]
- Anonymous credential systems [Camenisch,Lysanskaya'01,...]
- This talk: Fully Homomorphic Encryption (FHE) [Gentry'09,...]

Fully Homomorphic Encryption

- Encryption: used to protect data at rest or in transit

- Fully Homomorphic Encryption: supports arbitrary computations (F) on encrypted data



Leveled vs Full HE

- Leveled Homomorphic Encryption (LHE):
  - (pk,sk) $\leftarrow$ Gen(L)
  - Can compute $\mathrm{Eval}_{pk}(F,c)$ where F is a circuit of depth $\leq$ L
  - Can be build from standard LWE [Brakerski,Vaikuntanathan’11]
- Fully Homomorphic Encryption (FHE):
  - (pk,sk) $\leftarrow$ Gen()
  - $\mathrm{Eval}_{pk}(F,c)$ for arbitrary F
  - Still not known how to build from LWE
- Bootstrapping [Gentry’09]: Transform LHE $\rightarrow$ FHE
  - Requires LHE to be circular secure

FHE: state of the art

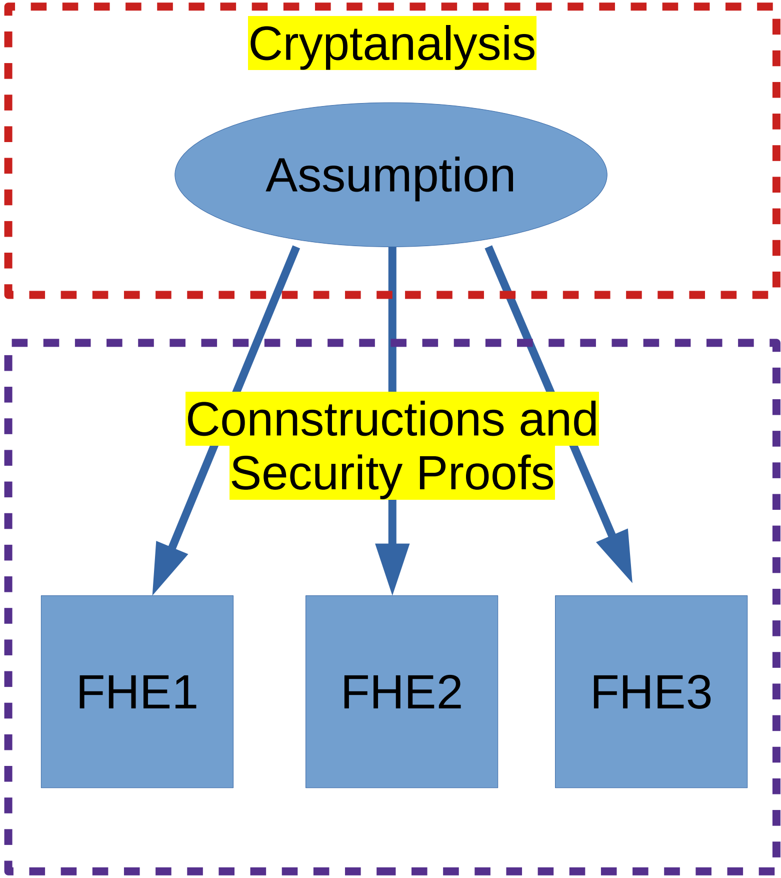
- Many FHE schemes based on LWE/RLWE [BV,BGV,BFV,GSW,DM,CGGI,…]
  - All use bootstrapping → require circular security
- Circular security
  - Has become a common “assumption” in FHE
  - No known attacks ...
  - … no cryptanalysis attempts
- Not considered here: schemes based on iO

The problem with circular security

- Circular security: "$\mathrm{Enc}_{pk}(f(sk))$ does not help"
  - Cannot even define before first defining Enc
  - encoding f(sk) depends on FHE Eval algorithm
  - Each scheme carries its own circular security assumption
- Hard to specify cryptanalysis challenges
- Similar "circular security" assumptions for iO were proposed and then broken

Our goal

- Formulate “LWE circular security” assumption(s)
- Advantages:
  - Simple, concrete assumption(s)
  - Allows to reduce multiple FHE schemes to the same (or small set of) assumptions
  - Supports reductions between assumptions
  - Basis to generate concrete challenges

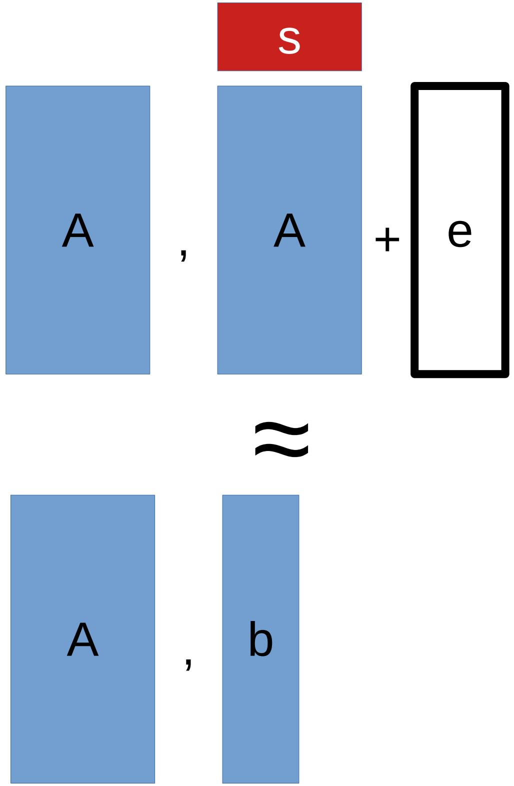


Contributions

- **Assumptions:** CircLWE, LinLWE, CliqueLWE
- **Reductions:** LinLWE $\leftarrow$ CircLWE $\leftrightarrow$ CliqueLWE
- **FHE:** BV,GSW, etc. are secure under CircLWE
- **Hardness:** LinLWE holds under LWE
- **Search-to-Decision** reduction for CircLWE
- **Robustness** of CircLWE under sk encoding
- **This is just a start:** much work still to be done

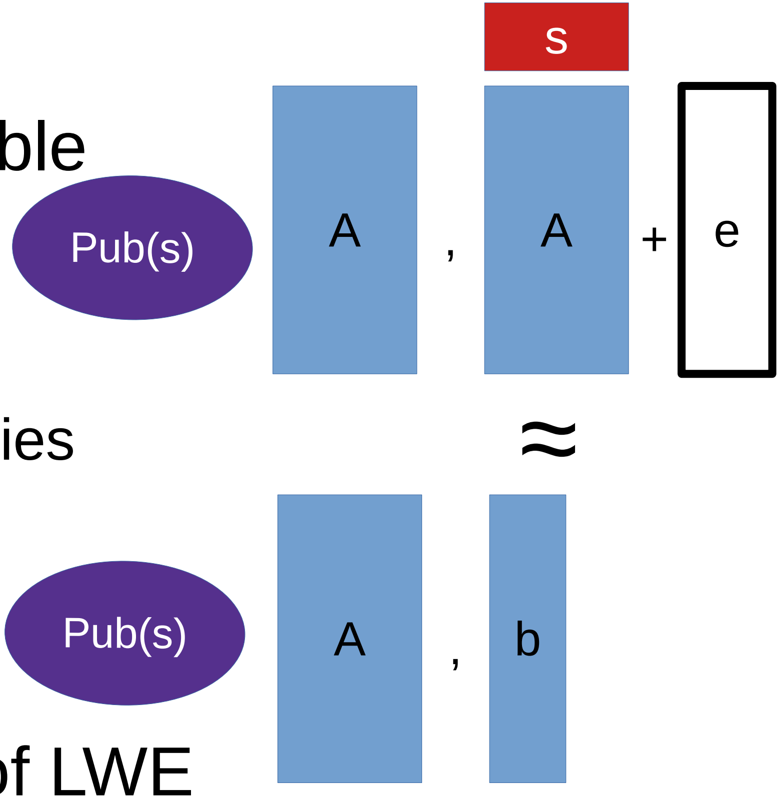
Learning With Errors (LWE)

- LWE Problem [Regev'05]
  - [A, As+e] ≈ [A, b] are indistinguishable
  - A,b ← uniformly random mod q
  - s: random secret vector
  - e ← random "error" vector with small entries
- LWE with side information Pub:
  - (Pub(s),[A, As+e]) ≈ (Pub(s),[A, b])
  - For lossy Pub: leakage resilience of LWE [Goldwasser,Kalai,Peikert,Vaikuntanathan'10]



Learning With Errors (LWE)

- LWE Problem [Regev'05]
  - [A, As+e] ≈ [A, b] are indistinguishable
  - A,b ← uniformly random mod q
  - s: random secret vector
  - e ← random "error" vector with small entries
- LWE with side information Pub:
  - (Pub(s),[A, As+e]) ≈ (Pub(s),[A, b])
  - For lossy Pub: leakage resilience of LWE [Goldwasser,Kalai,Peikert,Vaikuntanathan'10]



Matrix LWE

- Also known as “amortized LWE” [Peikert,Waters’08]
  - [A, AS+E] ≈ [A, B] where S,E,B are matrices
  - Follows from standard (single column) LWE by standard hybrid argument
- LWE with side information Pub:
  - (Pub(S),[A, AS+E]) ≈ (Pub(S),[A, B])
  - Follows from single column version if Pub works independently on the columns of S

Circular LWE

- For some (fixed, publicly known) function $\varphi: Z_q^n \rightarrow Z_q^m$
  - $[A, As+e+\varphi(s)] \approx [A, b]$
  - Equivalent to LWE when $\varphi(s)=Ps$ is linear
- Relating it to leakage (Pub) formulation:
  - $\varphi(s)=(\varphi'(s),0)$
  - $[A, As+e+\varphi(s)] = ([A_1, A_1s+e_1+\varphi'(s)] , [A_2, A_2s+e_2])$

    $= (\quad \text{Pub}(s) \quad , [A_2, A_2s+e_2])$
  - Pub(s) is an “LWE encryption” of $\varphi(s)$ under s

Circular LWE

- For some (fixed, publicly known) function $\varphi: Z_q^n \rightarrow Z_q^m$
  - $[A, As+e+\varphi(s)] \approx [A, b]$
  - Equivalent to LWE when $\varphi(s)=Ps$ is linear
- Relating it to leakage (Pub) formulation:
  - $\varphi(s)=(\varphi'(s),0)$
  - $[A, As+e+\varphi(s)] = ([A_1, A_1s+e_1+\varphi'(s)] , [A_2, A_2s+e_2])$
    $= (\quad \text{Pub}(s) \quad , [A_2, A_2s+e_2])$
  - Pub(s) is an "LWE encryption" of $\varphi(s)$ under s

Circular LWE

- For some (fixed, publicly known) function $\varphi: Z_q^n \to Z_q^m$
  - $[A, As+e+\varphi(s)] \approx [A, b]$
  - Equivalent to LWE when $\varphi(s)=Ps$ is linear
- Relating it to leakage (Pub) formulation:
  - $\varphi(s)=(\varphi'(s),0)$
  - $[A, As+e+\varphi(s)] = ([A_1, A_1s+e_1+\varphi'(s)] , [A_2, A_2s+e_2])$

    $= (\qquad \text{Pub}(s) \qquad , [A_2, A_2s+e_2])$
  - Pub(s) is an "LWE encryption" of $\varphi(s)$ under s

Strong CircLWE assumption

- For **any** function $\varphi: Z_q^n \rightarrow Z_q^m$: $[A, As+e+\varphi(s)] \approx [A, b]$
  - An even stronger assumption (for search LWE) was already proposed by [Canetti,Chen,Reyin,Rothblum'18]
- Is it equivalent to LWE for any φ?
- Can you find a φ for which it can be broken?
- Hard to give challenges!

  (cryptanalyst needs to choose φ first)
- What φ are relevant to FHE constructions?

Strong CircLWE assumption

- For **any** function $\varphi: Z_q^n \rightarrow Z_q^m$: $[A, As+e+\varphi(s)] \approx [A, b]$
  - An even stronger assumption (for search LWE) was already proposed by [Canetti,Chen,Reyin,Rothblum'18]
- Is it equivalent to LWE for any φ?
- Can you find a φ for which it can be broken?
- Hard to give challenges!

  (cryptanalyst needs to choose φ first)
- What φ are relevant to FHE constructions?

Lattice gadgets

- Gadget: (encG,decG,invG)
- Main example: powers-of-two gadget
  - encG(x) = (x, 2x, 4x, 8x,…, 2^kx)   for k = log q
  - invG(c) = binary decomposition of c
- Properties
  - Scalar product $\langle\langle$invG(c),encG(x)$\rangle\rangle$ = cx
  - decG(encG(x)+e) = x   for |e|<q/4
- Many other gadgets (CRT, Δ, hybrid, ...)

"Gadget LWE" Encryption

- secret key: $s \in Z_q^n$
- $gLWE_s(m) = [A, As+e+encG(m)] = [A,b] \bmod q$
- $Dec_s(A,b) = decG(b - As)$

  $= decG(encG(m)+e) = m$
- Corrects errors of size q<2, with message space $M=Z_q$
  - much better than scaling gadget $\Delta=q/p$ for $M=Z_p$
  - Can directly encrypt the secret key, ciphertexts, etc.

CircLWE

- $\mathrm{Pub}(s) = [A, As+e+\mathrm{encG}(\varphi(s))] = \mathrm{gLWE}_s(\varphi(s))$
- $\varphi(s) = \mathrm{invG}((1,s)) \times \mathrm{invG}((1,s))$
- If $s = s_0+2s_1+4s_2+ \ldots.$ with $s_i \in \{0,1\}^n$
  - $\varphi(s)=(1,s_0,\ldots,s_n,\ldots,s_i s_j,\ldots)$
- This is precisely the evaluation key of B12 FHE scheme
- **"Theorem":** B12 is secure under CircLWE
  - Proof: easy, by definition Pub(s)=evk of B12
  - This will be useful in proving other results

Search to Decision reduction

- Search CircLWE:
  - given [A, As+e+encG(φ(s))], find s
- Theorem: Search CircLWE is hard, then (decision) CircLWE is hard (for e' > 2^{λ} e)
- Proof:
  - Show how to "randomize" s
  - "Guess and check" the value of s, similar to standard search-to-decision reduction for LWE

Randomizing s in CircLWE

- $[A, As+e+G(\varphi(s))] = gLWE_s(\varphi(s)) = evk$
  - Want to map $s \rightarrow (s+r)$
  - $h_r([A,b]) = [A,b+Ar] = [A, A(s+r) + e + G(\varphi(s))]$
  - This is $gLWE_{r+s}(\varphi(s))$, not quite right
  - Let $f_r(\varphi(s))=\varphi(s+r)$, and use evk to compute

$$h_r(Eval_{evk}(f_r,evk)) = h_r(gLWE_s(\varphi(s+r)))$$
$$= gLWE_{s+r}(\varphi(s+r))$$

  - Add “smudging noise” to adjust the error distribution

Conclusion

- Strong LWE circular security:
  - pick your f, if you can break it let me know
- CircLWE for specific f:
  - relevant to FHE
  - nice properties, in theory
- CliqueLWE:
  - Pub = { $\mathrm{Enc}_{pk[i]}(sk[j])$: i,j}
  - equivalent to CircLWE
- Limitations:
  - blow up in error size
  - RLWE require additional information (automorphisms)
- This is just a start:
  - Much work still to be done
  - “CircLWE challenge page”?
- Practical FHE schemes?